

Firepower Management Center を使用した Firepower Threat Defense Virtual の管理

この章では、FMCを使用して管理されるスタンドアロンのFTDvデバイスを展開する方法について説明します。

(注)

本書では、最新の FTDv バージョンの機能を取り上げています。機能の変更の詳細について は、「Firepower Management を使用した Firepower Threat Defense Virtual の管理の履歴 (18 ページ)」を参照してください。古いバージョンのソフトウェアを使用している場合は、お使 いのバージョンの FMC 設定ガイドの手順を参照してください。

- Firepower Management Center を使用した Firepower Threat Defense Virtual について (1 ページ)
- Firepower Management Center $\sim \mathcal{O} \Box \mathcal{J} \mathcal{J} \mathcal{J}$ (2 $\sim -\mathcal{I} \mathcal{J}$)
- Firepower Management Center へのデバイスの登録 (2ページ)
- 基本的なセキュリティポリシーの設定 (5ページ)
- Firepower Threat Defense CLI へのアクセス $(17 \, \stackrel{\sim}{\sim} \stackrel{\scriptstyle \checkmark}{})$
- Firepower Management を使用した Firepower Threat Defense Virtual の管理の履歴 (18 ページ)

Firepower Management Center を使用した Firepower Threat Defense Virtual について

Firepower Threat Defense 仮想 (FTDv) は、Cisco NGFW ソリューションの仮想化コンポーネン トです。FTDv は、ステートフル ファイアウォール、ルーティング、VPN、Next-Generation Intrusion Prevention System (NGIPS) 、Application Visibility and Control (AVC) 、URL フィル タリング、高度なマルウェア防御 (AMP) などの次世代ファイアウォールサービスを提供しま す。 FTDv を管理するには、別のサーバ上で実行されるフル機能のマルチデバイスマネージャである Firepower Management Center (FMC)を使用します。FMC のインストールの詳細については、『FMCgetting started guide』を参照してください。

FTDvは、FTDv仮想マシンに割り当てた管理インターフェイス上のFMCを登録して通信します。

トラブルシューティングの目的で、管理インターフェイス上の SSH を使用して FTD CLI にア クセスすることも、Firepower CLI から FTD に接続することもできます。

Firepower Management Center へのログイン

FMC を使用して、FTD を設定および監視します。

始める前に

サポートされているブラウザの詳細については、使用するバージョンのリリースノート (https://www.cisco.com/go/firepower-notes)を参照してください。

手順

ステップ1 サポートされているブラウザを使用して、次の URL を入力します。

https://fmc_ip_address

• fmc_ip_address: FMC の IP アドレスまたはホスト名を指定します。

ステップ2 ユーザ名とパスワードを入力します。 ステップ3 [ログイン (Log In)]をクリックします。

Firepower Management Center へのデバイスの登録

始める前に

FTDv 仮想マシンが、正常に展開されていて、電源がオンになっており、最初のブート手順を 実行済みであることを確認してください。

手順

ステップ1 [デバイス (Devices)]>[デバイス管理 (Device Management)]を選択します。

ステップ2 [追加(Add)]ドロップダウンリストから、[デバイスの追加(Add Device)]を選択し、次の パラメータを入力します。 L

Host:+	
ftd-1.cisco.com	
Display Name:	
ftd-1.cisco.com	
Registration Key:*	
Group:	
None	•
Access Control Policy:* inside-outside	•
Smart Licensing	
✓ Malware	
Threat	
✓ URL Filtering	
Advanced	
Unique NAT ID:+	
natid56	
✓ Transfer Packets	

- •[ホスト(Host)]: 追加する論理デバイスの IP アドレスを入力します。FTD ブートスト ラップ設定で FMC の IP アドレスと NAT ID の両方を指定した場合は、このフィールドを 空のままにしておくことができます。
- [表示名(Display Name)]: FMC に表示する論理デバイスの名前を入力します。
- •[登録キー(Registration key)]: FTDv ブートストラップ設定で指定したものと同じ登録 キーを入力します。

- •[ドメイン (Domain)]:マルチドメイン環境を使用している場合は、デバイスをリーフド メインに割り当てます。
- •[グループ(Group)]: グループを使用している場合は、デバイスグループに割り当てま す。
- 「アクセスコントロールポリシー(Access Control Policy)]:初期ポリシーを選択します。
 使用する必要があることがわかっているカスタマイズ済みのポリシーがすでにある場合を 除いて、[新しいポリシーの作成(Create new policy)]を選択し、[すべてのトラフィック をブロック(Block all traffic)]を選択します。後でこれを変更してトラフィックを許可す ることができます。「アクセス制御の設定(15ページ)」を参照してください。

Name:	ftd_ac_policy		
Description:			
Select Base Policy:	None	~	
Default Action:	• Block all traffic O Intrusion Prevention	on 🔿 Network Discovery	

- [スマートライセンス (Smart Licensing)]:展開する機能に必要なスマートライセンスとして、[マルウェア (Malware)](AMP マルウェアインスペクションを使用する予定の場合)、[脅威 (Threat)](侵入防御を使用する予定の場合)、および[URL](カテゴリベースの URL フィルタリングを実装する予定の場合)を割り当てます。
- •[一意の NAT ID(Unique NAT ID)]: FTDv ブートストラップ設定で指定した NAT ID を 指定します。
- 「パケットの転送(Transfer Packets)]: デバイスから FMC へのパケット転送を許可します。このオプションを有効にして IPS や Snort などのイベントがトリガーされた場合は、 デバイスが検査用としてイベントメタデータ情報とパケットデータを FMCに送信します。 このオプションを無効にした場合は、イベント情報だけが FMCに送信され、パケットデー タは送信されません。
- ステップ3 [登録(Register)]をクリックし、正常に登録されたことを確認します。

登録が成功すると、デバイスがリストに追加されます。失敗した場合は、エラーメッセージが 表示されます。FTDv が登録に失敗した場合は、次の項目を確認してください。

ping: FTD CLI(「Firepower Threat Defense CLI へのアクセス (17 ページ)」) にアクセスし、次のコマンドを使用して FMC IP アドレスへの ping を実行します。

ping system ip_address

ping が成功しない場合は、show network コマンドを使用してネットワーク設定を確認しま す。FTD IP アドレスを変更する必要がある場合は、configure network {ipv4 | ipv6} manual コマンドを実行します。

- NTP:NTPサーバが[システム(System)]>[設定(Configuration)]>[時刻の同期(Time Synchronization)] ページの FMC サーバセットと一致することを確認します。
- ・登録キー、NAT ID、および FMC IP アドレス:両方のデバイスで同じ登録キーを使用していることを確認し、使用している場合は NAT ID を使用していることを確認します。
 configure manager add コマンドを使用して、FTDv で登録キーと NAT ID を設定することができます。また、このコマンドで FMC IP アドレスを変更することもできます。

基本的なセキュリティポリシーの設定

ここでは、次の設定を使用して基本的なセキュリティポリシーを設定する方法について説明します。

- 内部インターフェイスと外部インターフェイス:内部インターフェイスにスタティックIP アドレスを割り当て、外部インターフェイスに DHCP を使用します。
- DHCP サーバ: クライアントの内部インターフェイスで DHCP サーバを使用します。
- ・デフォルトルート:外部インターフェイスを介してデフォルトルートを追加します。
- •NAT:外部インターフェイスでインターフェイス PAT を使用します。
- •アクセスコントロール:内部から外部へのトラフィックを許可します。

手順

ステップ1 インターフェイスの設定 (5ページ) ステップ2 DHCP サーバの設定 (9ページ) ステップ3 デフォルトルートの追加 (10ページ) ステップ4 NAT の設定 (12ページ) ステップ5 アクセス制御の設定 (15ページ) ステップ6 設定の展開 (16ページ)

インターフェイスの設定

FTDv インターフェイスを有効にし、それらをセキュリティゾーンに割り当て、IP アドレスを 設定します。通常は、システムで意味のあるトラフィックを通過させるように、少なくとも2 つのインターフェイスを設定する必要があります。通常は、アップストリームルータまたはイ ンターネットに面した外部インターフェイスと、組織のネットワークの1つ以上の内部イン ターフェイスを使用します。これらのインターフェイスの一部は、Webサーバなどのパブリックアクセスが可能なアセットを配置する「緩衝地帯」(DMZ)となる場合があります。

一般的なエッジルーティングの状況は、内部インターフェイスでスタティックアドレスを定義 すると同時に、ISP から DHCP を介して外部インターフェイスアドレスを取得することです。

次の例では、DHCPによるスタティックアドレスとルーテッドモードの外部インターフェイス を使用して、ルーテッドモードの内部インターフェイスを設定します。

手順

- **ステップ1** [デバイス (Devices)]>[デバイス管理 (Device Management)]を選択し、デバイスの をク リックします。
- ステップ2 [インターフェイス (Interfaces)]をクリックします。

Overviev	v Analysis	Policies De	vices Obje	cts Al	1P Intel	ligence			(Deploy	0 ₄ System	n Help v	admin 🔻
Device M	anagement	NAT VPN	▼ QoS	Platform	Settings	FlexConfig	Certificates						
10.89. Cisco Firepo	.5.20 ower 9000 Serie	s SM-24 Threat De	efense									Save	🔀 Cancel
Device	Routing	Interfaces	Inline Sets	DHCP									
									🔍 Search by	name	Sync Dev	rice 🕜 Ado	d Interfaces 🔹
Inter	face	Logical Name	Туре		Security Zo	ones MAG	C Address (Activ	e/Standby)		IP Address			
🕅 Eti	hernet1/2		Physical									E <	Ø
🔂 Eti	hernet1/3.1		SubInter	face								Ξ	P
🚰 Et	hernet1/4	diagnostic	Physical									Ξ	Ø
😥 Eti	hernet1/5		Physical									Ξ	Ø

ステップ3 「内部」に使用するインターフェイスの をクリックします。

[全般(General)] タブが表示されます。

Edit Physical Interfa	ice					? >
General IPv4 IP	/6 Advanced	Hardware	Configuration			
Name:	inside				Enabled	Management Only
Description:						
Mode:	None					
Security Zone:	inside_zone	10.10		*		
Interface ID:	GigabitEther	net0/0	(64 - 9000)			
MTU:	1500		(01 5000)			
					OF	Cancel

a) 48 文字までの [名前 (Name)] を入力します。

たとえば、インターフェイスに inside という名前を付けます。

- b) [有効(Enabled)] チェックボックスをオンにします。
- c) [モード (Mode)]は[なし (None)]に設定したままにします。
- d) [セキュリティゾーン (Security Zone)]ドロップダウンリストから既存の内部セキュリティ ゾーンを選択するか、[新規 (New)]をクリックして新しいセキュリティゾーンを追加し ます。

たとえば、inside_zoneという名前のゾーンを追加します。各インターフェイスは、セキュ リティゾーンおよびインターフェイスグループに割り当てる必要があります。インター フェイスは、1つのセキュリティゾーンにのみ属することも、複数のインターフェイスグ ループに属することもできます。ゾーンまたはグループに基づいてセキュリティポリシー を適用します。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インター フェイスを外部ゾーンに割り当てることができます。この場合、トラフィックが内部から 外部に移動できるようにアクセスコントロールポリシーを設定することはできますが、 外部から内部に向けては設定できません。ほとんどのポリシーはセキュリティゾーンのみ サポートしています。NAT ポリシー、プレフィルタ ポリシー、および QoS ポリシーで、 ゾーンまたはインターフェイスグループを使用できます。

- e) [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。
 - •[IPv4]:ドロップダウンリストから[スタティックIPを使用する(Use Static IP)]を選 択し、IP アドレスとサブネットマスクをスラッシュ表記で入力します。

たとえば、192.168.1.1/24 などと入力します。

Edit Physical Interface							
General IPv4	IPv6 Advanced Hardware Configuration						
IP Type:	Use Static IP 💌						
IP Address:	192.168.1.1/24 eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25						

- •[IPv6]:ステートレス自動設定の場合は[自動設定(Autoconfiguration)]チェックボッ クスをオンにします。
- f) [OK] をクリックします。
- ステップ4 「外部」に使用するインターフェイスのをクリックします。

[全般(General)]タブが表示されます。

General IPv4 IPv	Advanced Hardware	e Configuration		
Name:	outside	-	Enabled	Management Onl
Description:]	
Mode:	None	•	 Image: A set of the set of the	
Security Zone:	outside_zone	•	-	
Interface ID:	GigabitEthernet0/0			
MTU:	1500	(64 - 9000)		
			0	K Cancel
48 文字までの [名]	前(Name)] を入力し	ます。		

- たとえば、インターフェイスに「outside」という名前を付けます。
- b) [有効(Enabled)]チェックボックスをオンにします。
- c) [モード (Mode)]は[なし (None)]に設定したままにします。
- d) [セキュリティゾーン (Security Zone)]ドロップダウンリストから既存の外部セキュリティ ゾーンを選択するか、[新規 (New)]をクリックして新しいセキュリティゾーンを追加し ます。

```
たとえば、「outside zone」という名前のゾーンを追加します。
```

e) [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。

- [IPv4]: [DHCPの使用(Use DHCP)]を選択し、次のオプションのパラメータを設定 します。
 - [DHCP を使用してデフォルトルートを取得(Obtain default route using DHCP)]: DHCP サーバからデフォルトルートを取得します。
 - •[DHCPルートメトリック(DHCP route metric)]:アドミニストレーティブディス タンスを学習したルートに割り当てます(1~255)。学習したルートのデフォ ルトのアドミニストレーティブディスタンスは1です。

Edit Physical Interface								
General	IPv4	IPv6	Advanced	Hardware	Configuration			
IP Type:			Jse DHCP					
Obtain def DHCP:	ault route	using 🧧	2					
DHCP route metric:		1	L	(1 - 255)				

- •[IPv6]:ステートレス自動設定の場合は[自動設定(Autoconfiguration)]チェックボッ クスをオンにします。
- f) [OK] をクリックします。
- ステップ5 [保存 (Save)]をクリックします。

DHCP サーバの設定

クライアントでDHCPを使用してFTDvからIPアドレスを取得するようにする場合は、DHCP サーバを有効にします。

- **ステップ1 [デバイス (Devices)]>[デバイス管理 (Device Management)]**を選択し、デバイスの をク リックします。
- ステップ2 [DHCP] > [DHCPサーバ(DHCP Server)]を選択します。
- ステップ3 [サーバ (Server)]ページで、[追加 (Add)]をクリックして、次のオプションを設定します。

Interface*	inside	*		
Address Pool*	10.9.7.9-10.9.7.25		(2.2.2.	10-2.2.2.20)
Enable DHCP Server				

- •[インターフェイス (Interface)]:ドロップダウンリストからインターフェイスを選択します。
- [アドレスプール(Address Pool)]: DHCP サーバが使用する IP アドレスの最下位から最 上位の間の範囲を設定します。IP アドレスの範囲は、選択したインターフェイスと同じサ ブネット上に存在する必要があり、インターフェイス自身の IP アドレスを含めることは できません。
- •[DHCPサーバを有効にする(Enable DHCP Server)]: 選択したインターフェイスの DHCP サーバを有効にします。
- ステップ4 [OK] をクリックします。
- ステップ5 [保存 (Save)]をクリックします。

デフォルトルートの追加

デフォルトルートは通常、外部インターフェイスから到達可能なアップストリームルータを指 し示します。外部インターフェイスにDHCPを使用する場合は、デバイスがすでにデフォルト ルートを受信している可能性があります。手動でルートを追加する必要がある場合は、次の手 順を実行します。DHCPサーバからデフォルトルートを受信した場合は、[デバイス (Devices)]> [デバイス管理 (Device Management)]>[ルーティング (Routing)]>[スタティックルート (Static Route)] ページの [IPv4ルート (IPv4 Routes)] または [IPv6ルート (IPv6 Routes)] テーブルに表示されます。

- **ステップ1** [デバイス (Devices)]>[デバイス管理 (Device Management)]を選択し、デバイスの をク リックします。
- **ステップ2** [ルーティング (Routing)]>[スタティックルート (Static route)]を選択し、[ルートを追加 (Add route)]をクリックして、次のように設定します。

Туре:	● IPv4 ○ IPv6		
Interface*	outside	~	
Available Net	work 🖒 🔘	Selected Network	
Search any-ipv4 Any-ipv4 Fv4-Enn Fv4-Linh Fv4-Linh Fv4-Priv Fv4-Priv F	chmark-Tests -Local ticast ate-10.0.0.0-8 ate-172.16.0.0 ate-192.168.0. ate-All-RFC191 Pv4-Relay-Anyı	Id	
Gateway*	default-gateway	 O 	
Metric:	1	(1 - 254)	
Tunneled:	Used only for default Route	:)	
Route Tracking:		~ ()	

- •[タイプ (Type)]: 追加するスタティックルートのタイプに応じて、[IPv4] または [IPv6] オプションボタンをクリックします。
- •[インターフェイス(Interface)]:出力インターフェイスを選択します。通常は外部イン ターフェイスです。
- [使用可能なネットワーク (Available Network)]: IPv4 デフォルト ルートの場合は [any-ipv4]、IPv6 デフォルトルートの場合は [any-ipv6] を選択します。
- [ゲートウェイ(Gateway)]または[IPv6ゲートウェイ(IPv6 Gateway)]:このルートのネ クストホップであるゲートウェイルータを入力または選択します。IPアドレスまたはネッ トワーク/ホストオブジェクトを指定できます。
- •[メトリック(Metric)]: 宛先ネットワークへのホップの数を入力します。有効値の範囲 は1~255 で、デフォルト値は1です。

ステップ3 [OK] をクリックします。

ルートがスタティックルートテーブルに追加されます。

Overview Analysis Policies	Devices Obj	ects AMP Int	elligence		Deploy	🕘 🌖 System	n Help √ ad
Device Management NAT	VPN VOS	Platform Settings	FlexConfig	Certificates			
.0.89.5.20 You have unsaved changes 🔡 Save 😢 Cance							
Device Routing Interfac	es Inline Sets	DHCP					
OSPF							O Add Route
OSPFv3	Network	Interface	Gateway	Tunneled	Metric	Tracked	
▷ 📁 BGP	▼ IPv4 Routes						
► Static Route	any-ipv4	outside	10.99.10.1	false	1		a 🖉
Multicast Routing	▼ IPv6 Routes						

ステップ4 [保存 (Save)] をクリックします。

NAT の設定

一般的な NAT ルールでは、内部アドレスを外部インターフェイスの IP アドレスのポートに変換します。このタイプの NAT ルールのことをインターフェイス ポート アドレス変換 (PAT) と呼びます。

- ステップ1 [デバイス (Devices)]>[NAT] をクリックし、[新しいポリシー (New Policy)]>[Threat Defense NAT] をクリックします。
- **ステップ2** ポリシーに名前を付け、ポリシーを使用するデバイスを選択し、[保存 (Save)]をクリックします。

Name:	interface_PAT	
Description:		
Targeted Devices		
Select device Available De	s to which you want to apply this policy vices	ted Devices
Search by	/ name or value	192.168.0.16
192.16	8.0.16	
	Add to Policy	
	Add to Folicy	

ポリシーが FMC に追加されます。引き続き、ポリシーにルールを追加する必要があります。

ステップ3 [ルールの追加(Add Rule)]をクリックします。

[NATルールの追加(Add NAT Rule)]ダイアログボックスが表示されます。

ステップ4 基本ルールのオプションを設定します。

Add NAT Rule			
NAT Rule:	Auto NAT Rule	~	
Type:	Dynamic	¥	I Enable
Interface Objects	Translation	PAT Pool	Advanced

- [NATルール (NAT Rule)]: [自動NATルール (Auto NAT Rule)]を選択します。
- ・[タイプ(Type)]:[ダイナミック(Dynamic)]を選択します。
- **ステップ5** [インターフェイスオブジェクト (Interface objects)]ページで、[使用可能なインターフェイス オブジェクト (Available Interface Objects)]領域から[宛先インターフェイスオブジェクト (Destination Interface Objects)]領域に外部ゾーンを追加します。

NAT Rule: Auto NAT Rule Type: Dynamic Dynamic Enable	Add NAT Rule						?
Type: Dynamic Constraints PAT Pool Advance Available Interface Objects C Source Interface Objects (0) Destination Interface Objects (1) Search by name Source Interface Objects (0) Destination Interface Objects (1) any Add to Source 2 Add to Destination 2 Add to	NAT Rule:	Auto NAT Rule	~				
Interface Objects Translation PAT Pool Advanced Available Interface Objects C Source Interface Objects (0) Destination Interface Objects (1) Search by name any 3 outside_zone Image: Control of Co	Type:	Dynamic	×	✓ Enable			
Available Interface Objects C Source Interface Objects (0) Destination Interface Objects (1)	Interface Objects	Translation	PAT Pool	Advanced	L		
Search by name any 3▲ outside_zone Add to Source 2 Add to Destination	Available Interface O	bjects 🖒		S	ource Interface Objects (0)	Destination Interface Objects (1)	
	inside_zone		A Sr 2 A Dest	dd to purce dd to ination	1179	3 🔊 outside_zone	

ステップ6 [変換 (Translation)]ページで、次のオプションを設定します。

Add NAT Rule			? ×
NAT Rule:	Auto NAT Rule		
Type:	Dynamic 💌 🗹 Enable		
Interface Objects	Translation PAT Pool Advanced		
Original Packet		Translated Packet	
Original Source:*	all-ipv4	Translated Source:	Destination Interface IP
Original Port:	ТСР 🗸		
		Translated Port:	

•[元の送信元 (Original Source)]:をクリックして、すべてのIPv4トラフィック (0.0.0.0/0) のネットワークオブジェクトを追加します。

Name	all-ipv4			
Description				
Network	O Host	O Range	Network	⊖ FQDN
Allow Override	s			

(注) 自動 NAT ルールはオブジェクト定義の一部として NAT を追加するため、システム定義のany-ipv4オブジェクトを使用することはできません。また、システム定義のオブジェクトを編集することはできません。

- [変換済みの送信元 (Translated Source)]: [宛先インターフェイスIP (Destination Interface IP)]を選択します。
- ステップ1 [保存 (Save)] をクリックしてルールを追加します。

ルールが [ルール (Rules)] テーブルに保存されます。

Overview An	alysis Po	licies Devices C	bjects AMP Int	elligence	16				Deploy 04 S	ystem Help	≠ admin v
interface		VPN V QOS	Platform Settings	FlexConfig C	ertificates			You	have unsaved change	s 📄 Save	Cancel
Enter Description											
Rules										Policy	Assignments (
Hilter by Device										0	Add Rule
					Original Pack	et		Translated Packet		1	
# Direction	Туре	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
▼ NAT Rules Befo	re										
▼ Auto NAT Rules											
# +	Dynamic	🥵 any	outside_zone	📄 all-ipv4			🥵 Interface			🍓 Dns:false	e 🥜 🗟
▼ NAT Rules Afte	r										

ステップ8 NAT ページで [保存 (Save)]をクリックして変更を保存します。

アクセス制御の設定

FTDvをFMCに登録したときに、基本の[すべてのトラフィックをブロック(Block all traffic)] アクセスコントロールポリシーを作成した場合は、デバイスを通過するトラフィックを許可 するためにポリシーにルールを追加する必要があります。次の手順では、内部ゾーンから外部 ゾーンへのトラフィックを許可するルールを追加します。他にゾーンがある場合は、適切な ネットワークへのトラフィックを許可するルールを追加してください。

より高度なセキュリティ設定とルールを設定する場合は、FMCの設定ガイドを参照してください。

- ステップ1 [ポリシー(Policy)]>[アクセスポリシー(Access Policy)]>[アクセスポリシー(Access Policy)]を選択し、FTDに割り当てられているアクセス コントロール ポリシーの をクリック します。
- ステップ2 [ルールを追加(Add Rule)]をクリックし、次のパラメータを設定します。

Add Rule											? ×
Name inside_to_out	side			🗹 Enat	bled	Insert	into Manda	tory			~
Action 🖌 Allow			▼ ∪ D ,2 t	5 D							
Zones Networ	ks VLAN Tags	🔺 Users	Applications	Ports	URLs	SGT/ISE Attribute	s		Inspection	Logging	Comments
Available Zones 🗳				Source	Zones (1)		Destina	tion Zones (1)		
🔍 Search by name				å.≜i	nside_zon	e	8	-ta 🛆 o	utside_zone		6
📇 🛕 inside_zone											
📇 📐 outside_zone											
			Add to Source								
			Add to Destination								

- •[名前(Name)]: このルールに名前を付けます(たとえば、inside_to_outside)。
- [送信元ゾーン (Source Zones)]: [使用可能なゾーン (Available Zones)]から内部ゾーン を選択し、[送信元に追加 (Add to Source)]をクリックします。
- [宛先ゾーン(Destination Zones)]: [使用可能なゾーン(Available Zones)] から外部ゾー ンを選択し、[宛先に追加(Add to Destination)] をクリックします。

他の設定はそのままにしておきます。

ステップ3 [追加 (Add)]をクリックします。

ルールが [ルール (Rules)] テーブルに追加されます。

Overview Analysis	olicies Dev	ices Objects	AMP Int	elligence							Dep	oloy 🔒	System Help 🛛	
Access Control + Access	Control Ne	twork Discovery	Application	n Detectors	Correlation	Actions v								
ftd_ac_policy You have unsaved changes Show Warnings Analyze Hit Counts Sove Soce									Cancel					
Prefilter Policy: Default Prefilt	er Policy			SSL	Policy: None				Identity Policy:	None				
											Te	Inheritance s	Settings 🖳 Policy Assign	ments (1)
Rules Security Intellige	Rules Security Intelligence HTTP Responses Logging Advanced													
# Filter by Device								Show Rul	e Conflicts 😡	Add Categ	jory 📀 Add Ru	le Search R	ules	×
Name #	Source Zo	Dest Zones	Source Ne	Dest Netw	VLAN Tags	Users	Applications	Source Po	Dest Ports	URLs	ISE/SGT A	Action	U 🗅 🕫 🕁 🔳 🛡	٠
▼ Mandatory - ftd_ac_policy (1-1)														
1 🛕 inside_to_outside	🚓 inside_zone	🚓 outside_zon	e Any	Any	Any	Any	Any	Any	Any	Any	Any	🖋 Allow	00.8000	a 🖉
▼ Default - Rd_ac_policy (-)														
There are no rules in this section. Add Rule or Add Category														
Default Action										Access 0	Control: Block All Tr	affic		×

ステップ4 [保存 (Save)] をクリックします。

設定の展開

設定の変更をFTDvに展開します。変更を展開するまでは、デバイス上でどの変更もアクティブになりません。

手順

ステップ1 右上の [展開 (Deploy)] をクリックします。



ステップ2 [ポリシーの展開(Deploy Policies)]ダイアログボックスでデバイスを選択し、[展開(Deploy)] をクリックします。

Dep	ploy Policies Version:2019-03-05 03:17 PM					? ×
	Device	Inspect Interruption	Туре	Group	Current Version	(j)
	■ 192.168.0.16	No	FTD		2019-02-28 07:11 AM	

ステップ3 展開が成功したことを確認します。展開のステータスを表示するには、メニューバーの[展開 (Deploy)]ボタンの右側にあるアイコンをクリックします。



Firepower Threat Defense CLI へのアクセス

FTDv CLIを使用して、管理インターフェイスパラメータを変更したり、トラブルシューティングを行ったりできます。CLIにアクセスするには、管理インターフェイスへのSSHを使用するか、VMware コンソールから接続します。

手順

ステップ1 (オプション1) FTDv 管理インターフェイスの IP アドレスに直接 SSH 接続します。

管理 IP アドレスは、仮想マシンを展開したときに設定したものです。初期展開時に設定した「admin」アカウントとパスワードを使用して FTDv にログインします。

ステップ2 (オプション2) VMware コンソールを開き、初期展開時に設定したデフォルトのユーザ名「admin」アカウントとパスワードを使用して ログインします。

I

Firepower Management を使用した Firepower Threat Defense Virtual の管理の履歴

機能名	プラット フォームリ リース	機能情報
FMC 管理	6.0	初期サポート。